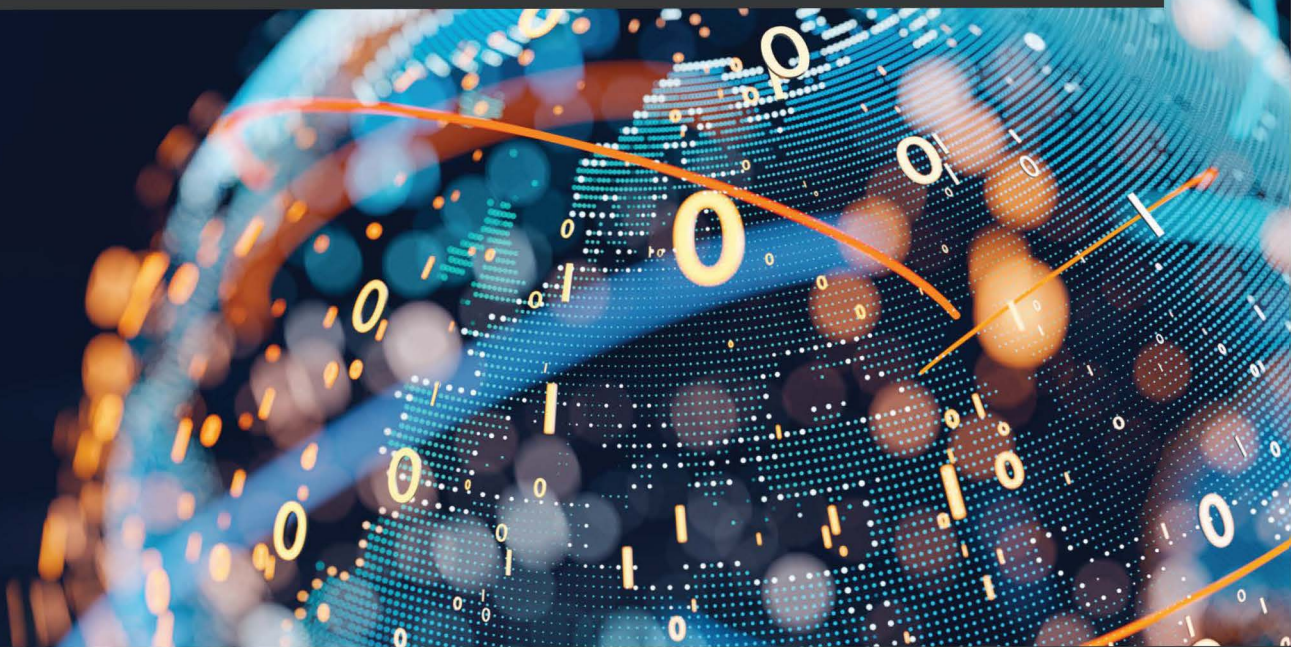


# Google Workspace User Guide

---

A practical guide to using Google Workspace apps efficiently while integrating them with your data



**Balaji Iyer**

Foreword by Abhi Jeevaganambi, CEO, Tradelytics



# Google Workspace User Guide

A practical guide to using Google Workspace apps efficiently while integrating them with your data

**Balaji Iyer**

**Packt**

BIRMINGHAM—MUMBAI

# Google Workspace User Guide

Copyright © 2022 Packt Publishing

*All rights reserved.* No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

**Associate Group Product Manager:** Alok Dhuri

**Publishing Product Manager:** Aaron Tanna

**Senior Editor:** Mark D'Souza

**Content Development Editor:** Rakhi Patel

**Technical Editor:** Simran Udasi

**Copy Editor:** Safis Editing

**Project Coordinator:** Rashika Shetty

**Proofreader:** Safis Editing

**Indexer:** Tejal Soni

**Production Designer:** Shankar Kalbhor

**Marketing Coordinator:** Anamika Singh

First published: March 2022

Production reference: 1180222

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

ISBN 978-1-80107-300-4

[www.packt.com](http://www.packt.com)

# 5

# Beyond Workspace

In the previous chapters, we extensively covered Google Workspace's core services and several add-on services in depth. This chapter will shed light on some of the non-core services and configuration options that extend Google Workspace's functionality via third-party apps and help reach a global audience of different categories and sizes.

Google is committed to making the world a better place, and true to its commitment, Google Workspace has products that target the younger generation and help them learn and comprehend the world around them. Google Classroom is one such product that integrates several core Workspace services into a seamlessly integrated platform, to enable student and teacher communication and collaboration.

In this chapter, we will cover the following topics:

- Google Classroom
- Google Marketplace apps and add-ons
- Google Assistant for Google Workspace
- Using third-party clients
- Accessibility settings

## Google Classroom

Google Classroom has been around for a few years now (since 2014, to be precise). However, the recent pandemic has accelerated the adoption of Classroom globally and pushed this service to more enterprise customers. Classroom has been traditionally used in educational institutions for teacher/student collaboration, but companies are now starting to use the platform for training employees and enabling their professional growth. Through native integrations with other services, such as Drive, YouTube, Slides, and Forms, Classroom allows content creators to make training sessions fun and interactive.

Google Classroom allows two sets of users to access content on the platform:

- **Teachers:** These users create classes, training material, and quizzes. They can grade answers and keep track of enrolled users' progress.
- **Students:** Those users who have enrolled in a course or class can access the material.

Google Classroom is bundled with Google Workspace for Education, which is a suite of easy-to-use tools that foster collaboration.

Google Workspace for Education is now available in four editions and depending on the needs and size of the organization, administrators can pick the edition that is right for them. The four editions of Google Workspace for Education, at the time of writing this book, are as follows:

- Google Workspace for Education Fundamentals
- Google Workspace for Education Standard
- Teaching and Learning Upgrade
- Google Workspace for Education Plus

### Old versus New

If you are familiar with G Suite offerings, then you will know that Google Workspace for Education Fundamentals was known as G Suite for Education and that Google Workspace for Education Plus was known as G Suite Enterprise for Education.

Google Education for Classroom Fundamentals edition is available globally to all qualifying educational institutions for free. To qualify for this free licensing, typically, educational institutions must be government-recognized and formally accredited. Once an application has been filed by the institution, Google determines the organization's eligibility to participate in the program and approves the application if all criteria are met successfully.

A comparison of the capabilities and features that are offered by the different Google Workspace for Education offerings can be found here: [https://edu.google.com/intl/ALL\\_us/products/workspace-for-education/editions/](https://edu.google.com/intl/ALL_us/products/workspace-for-education/editions/).

Now, let's move on to learning how to enable Google Classroom to take advantage of its great features, such as teacher and student classifications, setting up classes, enrolling students, managing grades and rosters, and unenrolling students.

## Enabling Google Classroom

Similar to the app configurations we saw in *Chapter 3, Application Security*, Google Classroom can be enabled for the entire domain or partially for a smaller subset of users. To enable Google Classroom as an administrator, follow these steps:

1. Log into the Google **Admin** console.
2. Click on **Apps** from the left-hand side panel.
3. Click on **Overview** to access **Additional Google services**.

The following screenshot shows the **Additional Google services** section in the **Apps** list:

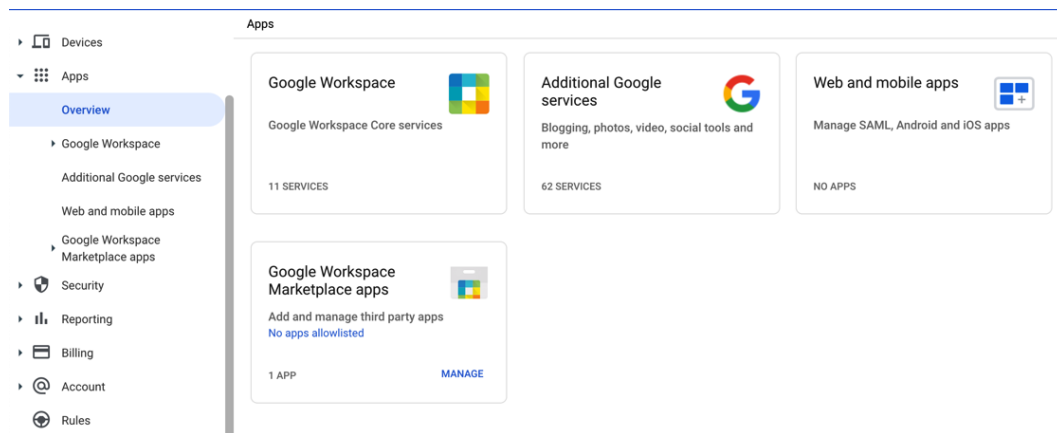


Figure 5.1 – Additional Google services in the Apps list

#### 4. Enable **Google Classroom** for the intended OUs or groups of users.

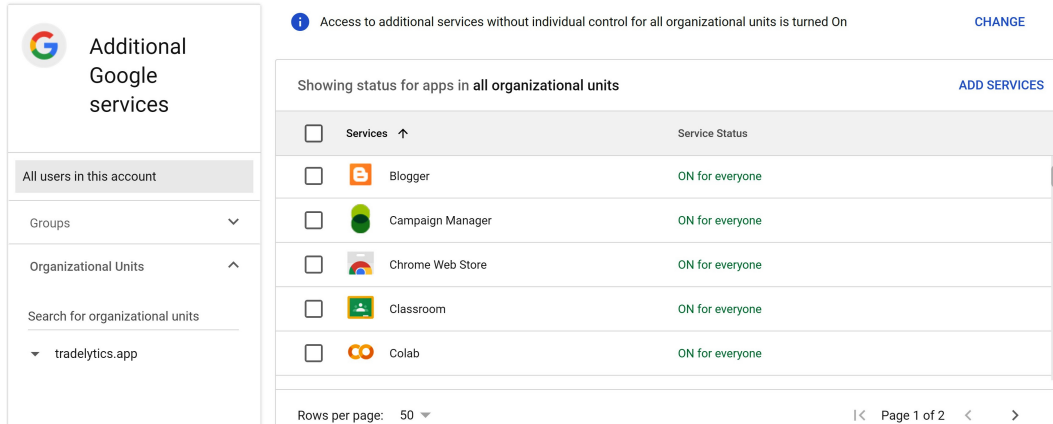


Figure 5.2 – Classroom in the list of Additional Google services

Once these entities have been enabled, users and trainers can access Google Classroom at `classroom.google.com` or from the **App Launcher** grid.

## Managing Google Classroom settings

The Google **Admin** console gives administrators several ways to configure and manage Google Classroom.

Users can typically sign into Google Classroom with one of the following user account types:

- School account
- Personal Google account
- Google Workspace account

Depending on the Google Workspace edition, users may be restricted to accessing content that is hosted in other domains, which would mean that not all users can join a class. Users' cross-domain access control policies typically determine whether they can access the content.

Google Classroom also controls access to certain services based on the age of the users. If users are under the age of eighteen, certain services will be disabled for those users.

The following screenshot shows the access settings that can be used to restrict or allow users from sharing their classes with users in other domains:

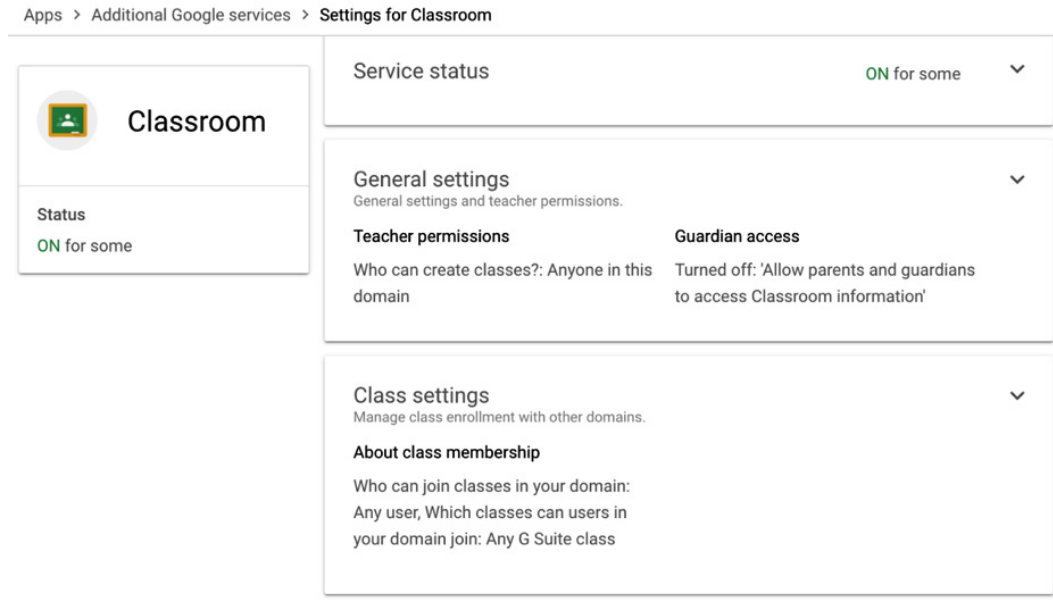


Figure 5.3 – Sharing settings for Google Classroom

We will look at each of these settings in the next few sub-sections.

## Teacher permissions

Google Classroom provides an intuitive way to classify users as teachers and students. When users sign into Google Classroom for the first time, they identify their role as either a **Teacher** or **Student**. When the user identifies themselves as a teacher, they are added to the **Teachers** group. Administrators can validate and give specific access to teachers, which allows them to create classes and view and manage guardians. The following screenshot shows what the **Teacher permissions** settings page looks like:

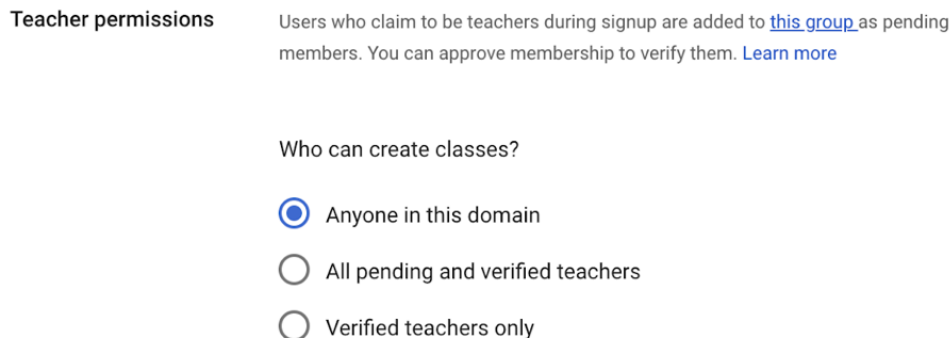


Figure 5.4 – Teacher permissions available in Google Classroom



**Important Note**

Once a teacher has created classes, caution should be exercised before deleting the teacher's account. Deleting a teacher's account before transferring ownership of classes to another teacher would limit functionality and would make the classes inaccessible.

**Guardian access**

For educational institutions, parents or guardians can be added to a class so that they can receive a class summary about the student.

This setting controls whether a parent or guardian can be granted access to a class and controls the elevated access granted to teachers. The following screenshot shows what the **Guardian access** settings page looks like:

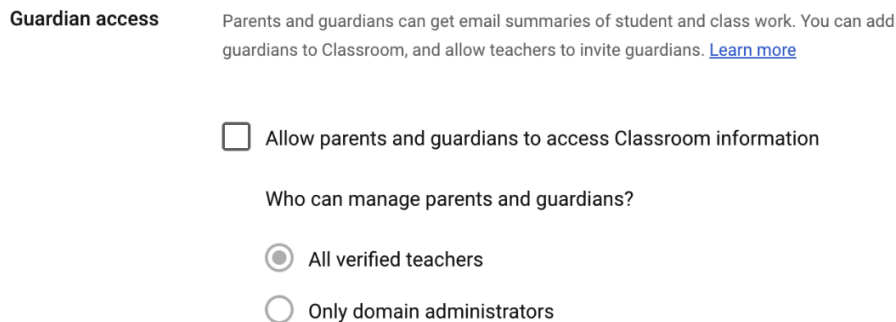


Figure 5.5 – Guardian access in Classroom

As you can imagine, with a large enrollment of students in a class, there would be a lot of guardians to invite or remove. Classroom makes it easy to invite guardians in bulk by importing a `.csv` file and manage them via the **Google Apps Manager (GAM)** tool.

**GAM**

GAM is a command-line tool for Google Workspace administrators to manage domain and user settings quickly and easily using the Workspace API. GAM requires a special service account that is authorized to act on behalf of the users to modify user-specific settings. More details on GAM can be found here: <https://github.com/jay0lee/GAM>.

**Class settings**

When the teachers are creating classes, students can be directly invited to join the class, or a class code is shared with the students who wish to enroll.

If organizations wish to keep this content secure, administrators can restrict who can join the class in Google Classroom. The following image shows the different options that are available for administrators:

#### About class membership

Allowing users to join classes from other domains will allow transfer of files into your domain.

Allowing users in your domain to join classes in other domains will allow transfer of files out of your domain. Files transferred out of your domain may be accessible to external users, and may be stored outside of your preferred data storage region. [Learn more](#)

#### Who can join classes in your domain

- Users in your domain only
- Users in whitelisted domains
- Any G Suite user
- Any user

#### Which classes can users in your domain join

- Classes in your domain only
- Classes in whitelisted domains
- Any G Suite class

Figure 5.6 – Class settings in Classroom

Trusted domains that frequently collaborate with the organization are added as whitelisted domains. You can either allow or restrict users from joining classes created by external domains. To allow users to join classes that have been created by trusted domains, you will have to whitelist them.

Since Google Classroom is well integrated with Google Drive and Meet, the content created in Classroom is stored in Google Drive. Access settings for Classroom determine if the content stored in Google Drive is accessible to external users.

Google Meet enables teachers to handle distance learning effectively. Teachers can create a unique Meet link for each class in Classroom. To help teachers manage meeting attendees, Meet links that are created in Classroom can be nicknamed. A teacher can control access to the video meeting, mute participants, prevent students from sharing their screen, and more.

### Nicknaming Links

Nicknaming links with Google Meet helps ensure that students don't rejoin a class meeting after the last participant has left the meeting. Typically, the last participant could be the teacher, and this prevents students from accessing Meet without a teacher present. Google Meet has more host controls for the education domain than other domains. The facility to nickname links is only available with Google Workspace for Education.

All editions of Google Workspace for Education, except for Google Workspace for Education Fundamentals, allow teachers to generate an attendance report at the end of a meeting.

Grades and rosters are essential functions in any classroom setup, so let's look at them in the next section.

## Grades and rosters

Grades for quizzes and assignments can be exported for all the students in a class. This information can then be imported into **School Information Systems (SISs)** to reflect in respective educational tracking systems.

Educational institutions can enable classroom roster information to sync to the SIS, called **Clever**. To navigate to **Roster import**, go to **Google Admin Console | Settings for Classroom | Roster import**.

The **Roster import** option must be turned on before data can be integrated with Clever. However, educational institutions that need this integration would need to have a Google Workspace for Education Plus license.

More details on Clever and how it handles rostering can be found here: [https://support.clever.com/s/articles/000001463?language=en\\_US](https://support.clever.com/s/articles/000001463?language=en_US).

## Student unenrollment

Just like students can enroll in a class, administrators can configure who can unenroll students from a class. Typically, educational institutions may not want students to unenroll themselves to avoid problems with the class roster. Further, students may unenroll themselves for fun. So, it would be better if teachers could control the unenrollment process. This can be achieved via the **Student unenrollment** setting in the Google **Admin** console.

To access this setting as an administrator, Navigate to **Student unenrollment** using the following path: log into the Google **Admin** console | **Apps** | **Google Workspace** | **Setting for Classroom** | **Student enrollment**:

The screenshot shows the 'Student unenrollment' settings page. At the top, there is a header 'Student unenrollment' with an upward-pointing arrow. Below this, the 'Unenrollment permissions' section is visible, with a sub-header 'Unenrollment permissions' and a note 'Applied at 'tradelytics.app''. The main setting is 'Who can unenroll students from classes?', which has two radio button options: 'Students and teachers' (selected) and 'Teachers only' (unselected). Below the 'Teachers only' option, there is a note: 'Students will need to ask teachers to unenroll them'. At the bottom of the settings area, there is an information icon (i) and a note: 'Most changes take effect in a few minutes. Learn more' and 'You can view prior changes in the Audit log'. At the very bottom right of the page, there are 'CANCEL' and 'SAVE' buttons.

Figure 5.7 – The Student unenrollment setting

Under **Who can unenroll students from classes?**, select **Students and teachers**. After this step, students will not be able to unenroll themselves and only teachers or administrators will be able to perform the action

As we can see, Google Workspace is feature-rich, secure, easy to use, and seamless when it comes to collaboration in educational institutions. Its popularity is always increasing, and the free version has made it easier for people in different regions of the world to take advantage of these features. With Google Classroom taken care of, let's move on and talk about Marketplace apps in detail.

## Google Workspace Marketplace apps

We gave a brief introduction to Marketplace apps in *Chapter 2, Configuring Users and Apps*, where we covered the intent behind these apps and some of the popular Marketplace apps. In this section, we will talk about how to install and manage Marketplace apps across the userbase as an administrator. We will also talk about add-ons and how they integrate with some of the core services. This will be followed by a deeper look at access control for third-party applications, which enables administrators to keep Workspace data and users secure.

**Important Note**

As you may recall, Marketplace apps are applications developed by aspiring developers or product owners trying to integrate their product with Google Workspace and help extend the tool set's functionality beyond Google Workspace.

As an organization with multiple functional groups, there may be several business needs and workflows to solve daily. While Google Workspace tries to solve several of them, Marketplace apps fill in the gaps where Google Workspace services are not available just yet. To make it easy to work with and integrate Marketplace apps, **Security Assertion Markup Language (SAML)** authentication is supported within Google Workspace, making Google Cloud Identity the primary identity provider.

There are several notable workflows that Marketplace apps help with. For instance, users can use an e-signature app with Drive to initiate a document for an e-signature workflow.

Another example would be users opening a support ticket notification email to see relevant support ticket information populating the side panel within the Gmail page. This information will be fetched from the case management app hosted in Google Marketplace.

Based on whether the application is developed by your organization or by a third-party developer, it can be published internally within the organization or added to the allowed list of apps that users can install.

To add a Marketplace app to a list of approved apps that users can install, follow these steps:

1. Log into the Google **Admin** console.
2. Click on **Apps** from the left-hand side panel and select **Google Workspace Marketplace Apps**.
3. Click on **Add app to Domain Install list**.
4. Use the **Browse** option to select relevant apps for installation.
5. Install the app using one of the following options:
  - **Individual Install:** This installs the app just for the logged-in user's account.
  - **Domain Install:** This option installs the app for all the users in the domain.

Once the app has been installed, users can start using the app right away. Sometimes, app owners may choose to enforce licenses when using an app. Administrators may have to procure licenses for app usage.

The following screenshot shows the section in the Google **Admin** console where apps could be added to the **Domain Install** list:

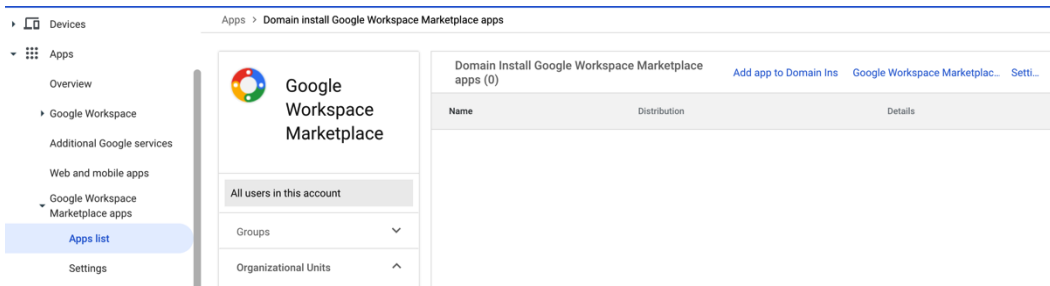


Figure 5.8 – Adding third-party applications to the Domain Install list

Installed Marketplace apps can surface on multiple locations within Google Workspace. Here are some examples of where the apps can surface:

- In the **Google Docs/Sheets/Slides** page via the **Add-Ons** menu:

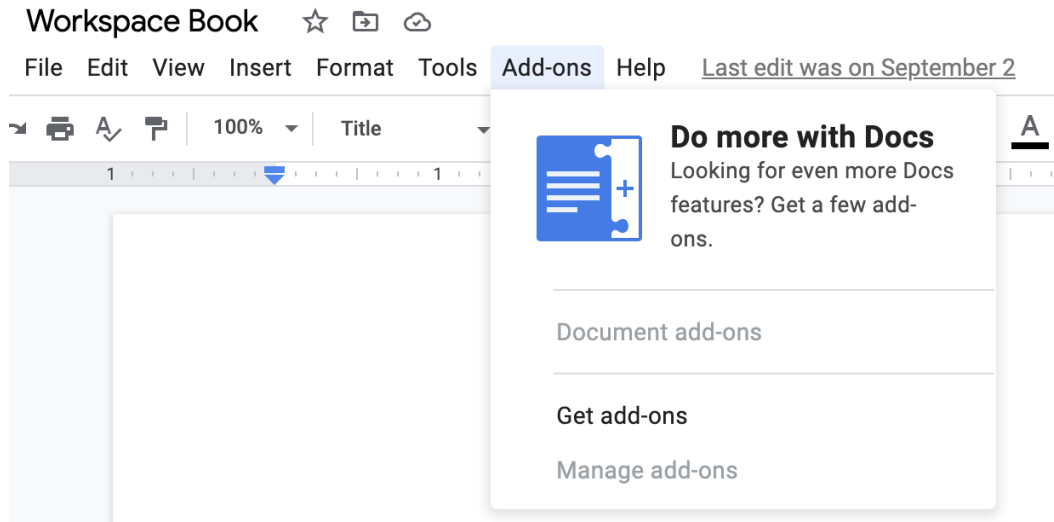


Figure 5.9 – Marketplace apps via Add-ons with Google Docs

- In the Google Drive home page through the **File** menu option.

- Through the **App Launcher** icon, you need to scroll past listed core services to get to the Marketplace apps listed there:

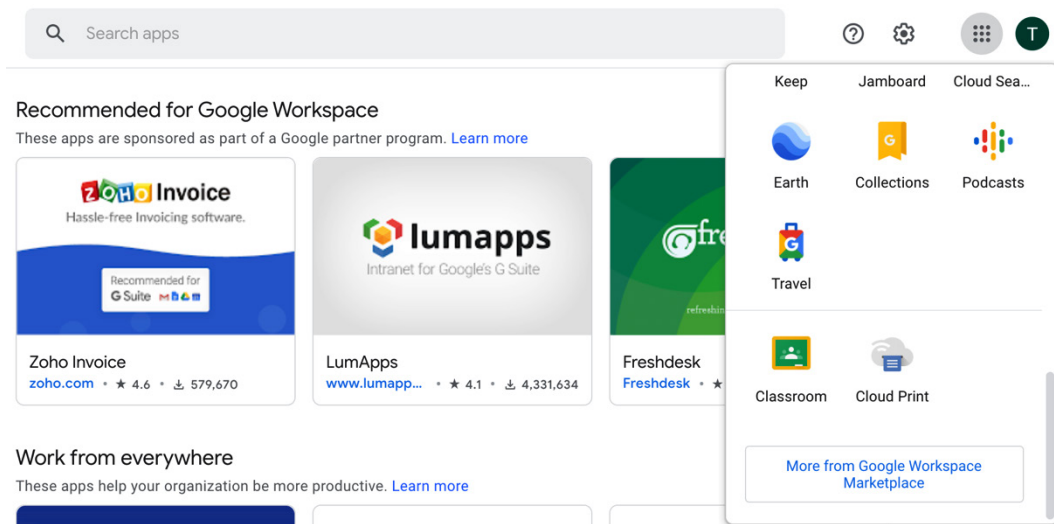


Figure 5.10 – Navigating to Marketplace apps using the App launcher icon

The ability to restrict the installation of Marketplace apps improves a domain's security posture tremendously by not allowing installation of non-curated applications that may be harmful.

## Managing Marketplace apps

While the installation of a Marketplace app sounds straightforward, organizations may want to restrict users from installing multiple apps in their domain. Google Workspace provides the option of completely restricting users from installing any app.

If users are restricted from installing any app, administrators can create a curated list of apps that are allowed for installation within the domain. Users can only pick apps from this list for their use.

You can navigate to the **Marketplace Settings** page to make these adjustments by following these steps:

1. Log into the Google **Admin** console.
2. Click on **Apps** from the left-hand side panel and select **Google Workspace Marketplace Apps**.

3. Click on **Settings**. From here, you can choose whichever setting you want:

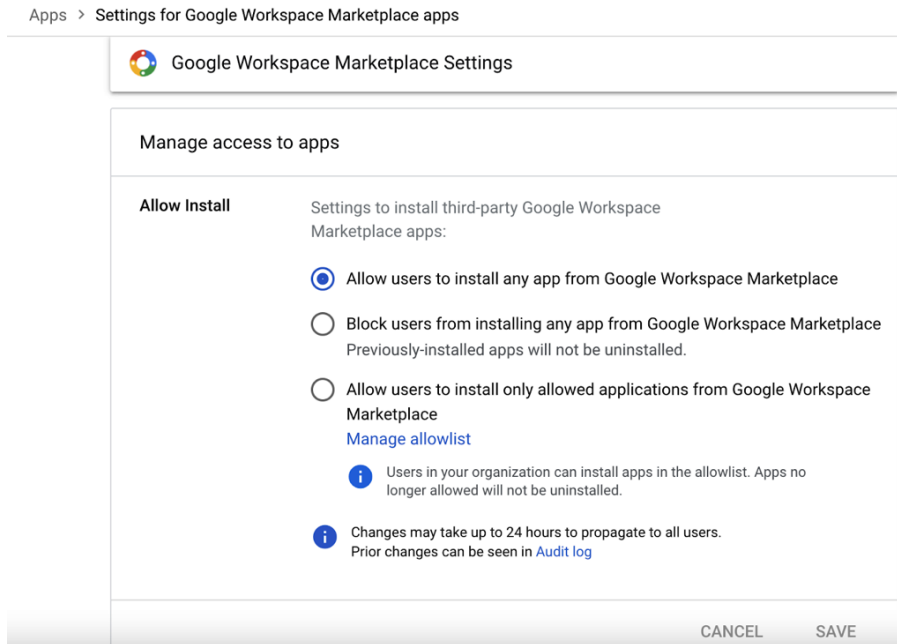


Figure 5.11 – Marketplace apps settings for administrators

Google Workspace also has add-ons, which are remarkably similar to third-party Marketplace applications, the purpose of which is to augment the capabilities core Google Workspace services already offer.

Add-ons differ from third-party applications in terms of how they are discovered and installed. Add-ons can be browsed directly from Google Workspace services by clicking the **Add-ons** tab on each service. Service-specific add-ons show up across these core services. Many of these add-ons are developed by third parties but they are seamlessly integrated with Workspace services. We'll learn how to enable and work with these add-ons in the next section.

## Add-ons for Google Workspace services

In this section, we will look at add-ons and some representative examples of using them across Google Workspace core services such as Drive, Docs, Sheets, and Calendar.

Users can use the add-ons that have been installed by an administrator from their Google Drive. Furthermore, there is an option for users to install add-ons individually via the Google Docs editor.



This can be allowed or restricted from the Google **Admin** console, as follows:

1. Log into the Google **Admin** console.
2. Click on **Apps** from the left-hand side panel and select **Google Workspace | Drive and Docs | Features and Applications | Add-ons**.

This setting allows you to enable or disable add-on installation, as per the OU:

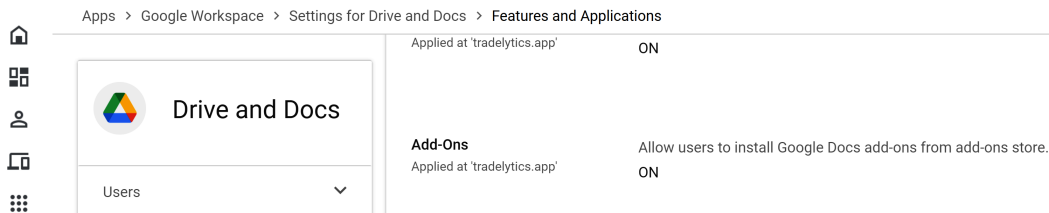


Figure 5.12 – Enabling/disabling add-ons

Once enabled, add-ons can be accessed from the Drive, Gmail, and Calendar home pages through the right-hand side panel using the + icon:

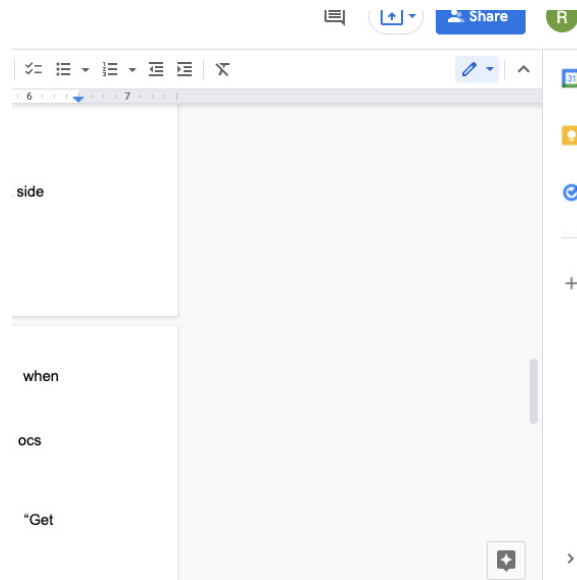


Figure 5.13 – The + icon in Docs, which helps install add-ons

When add-on installation is allowed, users can use the **Add-ons** menu from the Document editor and use the **Get Add-ons** option to browse the available and compatible add-ons for their business needs.

Due to how seamlessly add-ons can be integrated with Workspace services, add-ons can be used to surface contextual information that's specific to the application you are working on. Let's look at a couple of representative examples of how add-ons can be beneficial across some popular Workspace services.

The following image shows the add-ons that are available for Google Docs:

The screenshot shows the Google Workspace Marketplace interface. At the top, there is a search bar labeled "Search apps" and several utility icons. Below the search bar, the text "Works with Docs" is followed by the subtitle "These apps can be used directly with Docs to improve your productivity." The main content area displays a grid of eight add-on cards, each with a header image, title, developer name, description, and user ratings.

Add-on Name	Developer	Description	Rating	Downloads
MathType	WIRIS	Easily write math equations	★ 4.0	10,000,000+
Lucidchart Diagrams	Lucid Software	Lucidchart provides collaborative online diagramming to make it easy t...	★ 3.9	10,000,000+
Doc To Form	Oli Trussell	Doc To Form allows you to quickly and easily create a form from text within a Google Doc.	★ 3.8	10,000,000+
EasyBib Bibliography Cr...	EasyBib	The easiest automatic bibliography citation generator is now on Google Docs! Forma...	★ 3.6	10,000,000+
Hypatia Create	Hypatia Systems Inc.	Finally, a fast and easy way to include math equations in Google Docs, Slides, and Form...		
Easy Accents - Docs	Daniel Baker	This Add-on allows users to easily insert accents for different languages directly...		
Kaizena	engineering	Kaizena helps teacher provide fast, high-quality feedback on student work		
Automagical Forms	Unicorn Magic	Automagically convert your PDFs, Docs, and Slides to Google Forms™.		

Figure 5.14 – List of add-ons for Google Docs

Let's look at an example of using add-ons from Google Sheets using the *Salesforce* add-on. By installing the **Salesforce** add-on, users can start using the data integration capability across Salesforce and Google Sheets. To make this happen, administrators should enable add-on installation for users or add the Salesforce app to the allowlist. Users can then install the add-on.

Then, users can open a Google Sheet and use the **Extensions** option to create a data connector for Salesforce. This connector can be used to import a report from Salesforce into Google Sheets or to write a query to pull data from Salesforce into Google Sheets.

Google Sheets can help derive intelligence and insights on the data that's been pulled from Salesforce. In a bi-directional flow, when data in Google Sheets is updated, changes get reflected in Salesforce as well through this data connector.

Like Drive add-ons, administrators can install the relevant add-ons for Gmail and Calendar as well. The following screenshot shows some of the add-ons for Calendar:

The screenshot displays the Google Workspace Marketplace interface for 'Works with Calendar' add-ons. The page is titled 'Works with Calendar' and includes a search bar for 'Search Calendar Add-ons'. Below the title, there are eight add-on cards, each with a logo, name, description, and user ratings/downloads.

Add-on Name	Description	Rating (Stars)	Downloads
GoToMeeting	GoToMeeting Video Conferencing... Seamlessly schedule, flawlessly manage and easily join upcoming meetings directly...	3.8	1,472,098
Box for Google Workspace	Seamlessly copy your Google files over to Box, attach files to emails from Box, and download...	4.4	783,461
Attendance Taker for Classroom	Designed for teachers, Attendance Taker for Classroom makes tracking attendance...	4.2	720,969
Streak CRM for G Suite	Streak is the premier G Suite-integrated CRM	3.9	681,564
SMS Reminder for Google	SMS Reminder is a Google Calendar™ add-on that allows you to set appointment...	-	-
Wrike for Google Workspace	Create Wrike tasks from emails, easily pick assignees from list of suggestions. Search, view and...	-	-
Dialpad Meetings for Google	Schedule calls from Google Calendar and easily access your call info.	-	-
RingCentral Addon	The RingCentral Addon makes communicating with email and calendar easier.	-	-

Figure 5.15 – List of add-ons for Calendar

For example, when users search for add-ons in the Calendar UI, Google Workspace Marketplace displays specific add-ons that are compatible with Calendar data. Add-ons such as **SMS Reminders**, **Dialpad Meetings**, and **GoToMeeting** will show up in the search results.

All these add-ons, which have been published on Google Workspace Marketplace, go through a detailed security review before being approved for usage across all domains. This security review is a very critical step as these add-ons seamlessly integrate and look like they are developed by Google, giving users a false sense of security. Caution must be exercised when users work with third-party apps and add-ons.

When a third-party application is installed, it will request several permissions for accessing your Google Workspace data. These may include the following:

- View and manage your contacts
- Share documents with others
- Connect to third-party services to read/write data
- Send emails on behalf of users

These are very sensitive and critical functions that users should not typically trust a third-party application with by default. Administrators and users should join forces to restrict application access to keep their Workspace data secure. The next section will describe how granular access can be granted to third-party applications using Auth scopes and the OAuth 2.0 protocol.

## Access control for third-party applications

Administrators can control which third-party applications can access Google Workspace data. Access control for applications is defined using the OAuth 2.0 protocol, which is a mechanism that controls an application's access to the user's account. Administrators can choose to do any of the following:

- Restrict access to Google Workspace services
- Give unrestricted access to Google Workspace services
- Trust specific applications with data
- Trust all domain-owned applications

Follow these steps to accomplish the preceding options:

1. Log into the Google **Admin** console.
2. Select **Security**, followed by **Access and data control**, and then **API Controls**.
3. Under **App Access Control**, select **MANAGE THIRD-PARTY APP ACCESS**:

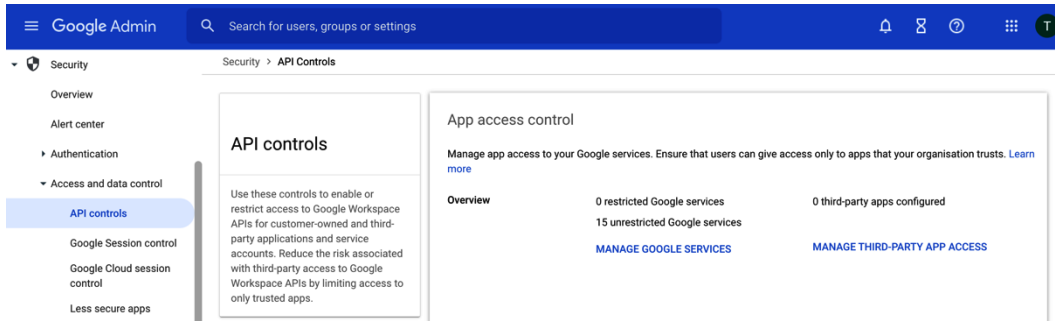


Figure 5.16 – Security option to set app access control for third-party apps

4. From the list of apps, Select applications to change accesses, then choose **Change access**:

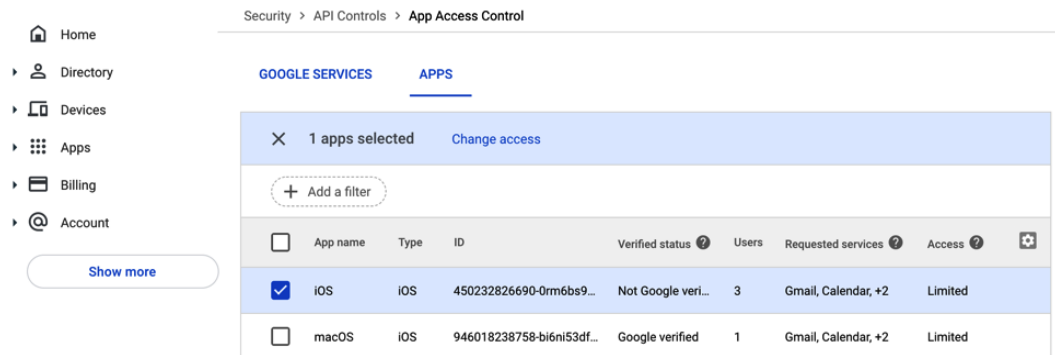


Figure 5.17 – The Change access option for third-party applications

5. Select either **Trusted**, **Limited**, or **Blocked**:

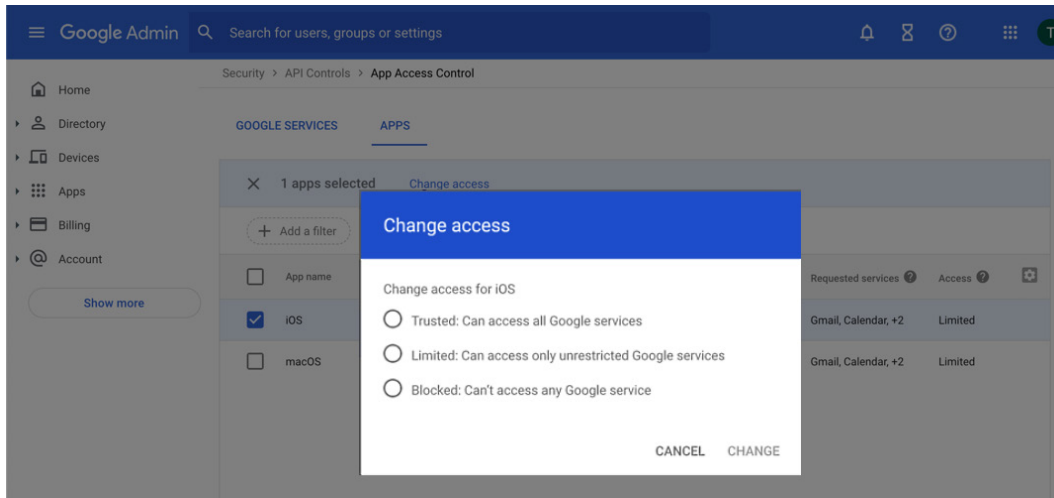


Figure 5.18 – Options for changing access for third-party applications

6. Click **CHANGE**.

**Trusted** third-party applications will be allowed to access all Google services, while **Blocked** applications cannot access any services at all. **Limited** third-party applications find common ground, which allows administrators to pick and choose between Google services that a Marketplace application will be allowed to access.

Several third-party applications typically request a lot of overarching permissions and will request access to data that may not be needed. Google Workspace provides a nifty way to handle such applications using APIs and OAuth scopes.

Using an **application programming interface (API)** is an intermediary option that allows programmable access to data sources. Developers use APIs to programmatically access data across Google Workspace. Auth scopes express the permissions you request to users to authorize your apps.

The following are some examples of Auth scopes:

- Use the Gmail API, `messages.list()`, to list all the messages for a particular user.
- Use the Drive API, `driveService.files().create()`, to create Drive files programmatically.

Third-party apps can integrate with Google Workspace using Google Workspace APIs. Using your app settings, the level of data access these apps can have is controlled via scopes. The following steps show how to configure scopes for Marketplace applications:

1. Log into the Google **Admin** console.
2. Click on **Apps** from the left-hand side panel and select **Google Workspace Marketplace Apps**.
3. Upon selecting the app, you will see the following page:

Apps > Domain install Google Workspace Marketplace apps > AODocs

Configuration for AODocs - Google Workspace Marketplace

**Distribution**

Enabled for all organizational units.  
[View organizational unit](#)

**Data Access**

Status: Granted [Grant access](#) [Revoke access](#)

[OAuth Scopes](#) [OAuth Clients](#)

These are the Google service APIs (OAuth scopes) that AODocs is requesting.

[EXPAND ALL](#) [COLLAPSE ALL](#)

Figure 5.19 – Auth scopes for Marketplace apps

Here's what the options seen in the preceding screenshot control:

- **Distribution:** This controls whether the apps are enabled or disabled for the selected OU. Like any app settings, the controls are inherited from the parent/root OU. This can be overridden with a different setting for each nested sub-OU.
- **Data Access:** This controls the API scopes the app has access to.

Users must authorize access scopes for an app when they are run the first time. For example, an app may want permission to create events in a calendar. By selecting a specific granular scope, users can ensure that the app cannot do anything other than create events in your calendar.

At any point in the future, if an app is no longer required, it can be deleted. All associated licenses related to the app will also be removed.

Apps that have been created by internal employees of the domain or any external developers may interact with Google Workspace using an API. Administrators can evaluate an app to check what scope of access is required for this application to function. Developers generally follow best practices to use restricted scopes that are required for the application and do not use scopes that are not required for the application.

For instance, the following are some examples of Gmail scopes:

- `https://www.googleapis.com/auth/gmail.insert`
- `https://www.googleapis.com/auth/gmail.modify`
- `https://www.googleapis.com/auth/gmail.readonly`
- `https://www.googleapis.com/auth/gmail.send`

These scopes are very intuitive and give extremely specific access to Gmail data. Some scopes are categorized as **Recommended**, **Sensitive**, or **Restricted**.

The following steps will help administrators navigate and review the scope of each Marketplace application installed in the domain:

1. Log into the Google **Admin** console.
2. Click on **Security** from the left-hand side panel and select **API Controls**.
3. Click on **Manage Third-Party App Access**.



This lists the following details about the app:

- **App Name**
- **ID**
- **Verified Status:** Apps that are validated by the Google Security team are listed as verified.
- **Type**
- **Users:** This shows the number of users using this app.
- **Access** shows **Limited**, **Trusted**, or **Blocked**. The preceding steps are very similar to what was described in *Figure 5.15* and *Figure 5.16*.

4. Click on the app for more details on its scopes:

The screenshot displays the Google Admin console interface. On the left, a navigation menu includes 'Directory', 'Devices', 'Apps', 'Billing', and 'Account', with a 'Show more' button below. The main content area is divided into two sections: 'App Status' and 'Requested Services'. The 'App Status' section shows 'Verified status' as 'Google verified'. The 'Requested Services' section, titled 'These are the Google service APIs (OAuth scopes) that macOS is requesting.', includes 'EXPAND ALL' and 'COLLAPSE ALL' links. Below this is a table listing requested services:

Service	Scopes
Gmail	1 scope
Calendar	1 scope
Contacts	1 scope
Other	3 scopes

At the bottom left, there is a 'Send feedback' button and copyright information: '© 2021 Google Inc. Terms of service - Billing terms - Privacy Policy'.

Figure 5.20 – The Google Admin console showing scopes for a Marketplace app in a collapsed view

5. From the **App details** page, review the API scopes that have been requested by the app.

## 6. Expand the scopes to see the detailed list:

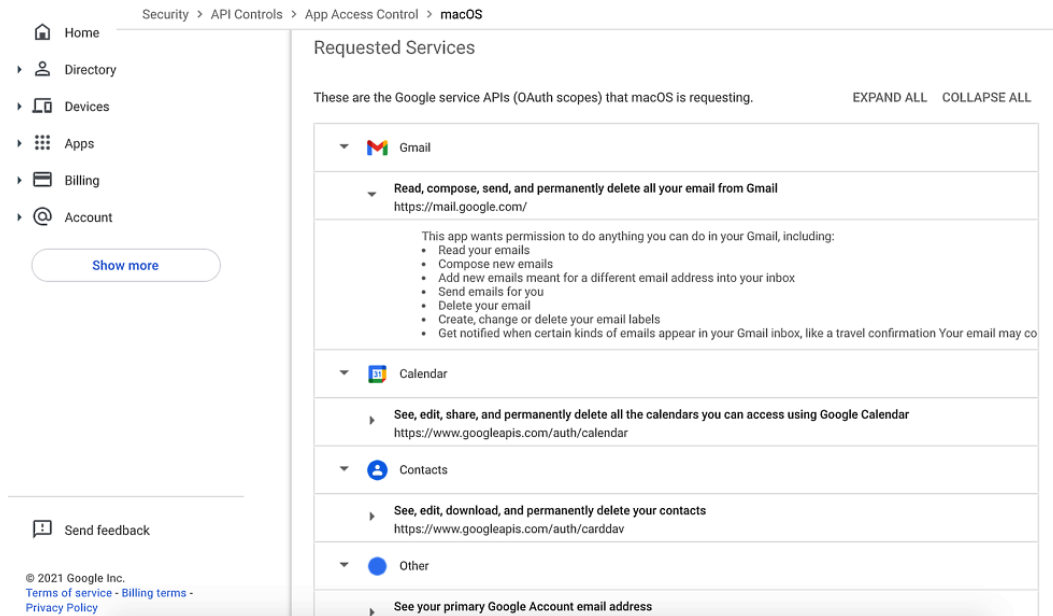


Figure 5.21 – The Google Admin console showing scopes for a Marketplace app in an expanded view

On the same page, after reviewing the list of OAuth API scopes, administrators can make an informed decision regarding whether to allow or restrict access to this application.

To change access to the scope of an application, administrators can follow these steps:

1. Click on **Manage Google Services** and look at the list of Google services that can be controlled from the Google **Admin** console.
2. Select the service that needs to be changed and click on **Change Access**.
3. Review the list of OAuth scopes and apply the changes.

Once the changes have been applied and the OAuth access level has been updated, users who are using the app will see the changes being reflected immediately. If an existing app is changed to have a "restricted" scope, then it will stop working for users using the app. Similarly, apps that are blocked can no longer be installed.

To make it easy for users to understand the changes that have been implemented, administrators can post a user-friendly error message when an app's access is changed. To accomplish this, the admin can do the following:

1. Navigate to the **App Access control** section within the Google **Admin** console and click on **Settings**.
2. Enter the customized error message in the text box provided.
3. Click **SAVE**.

In the next chapter, we will learn how to create customized third-party applications using developer tools such as Apps Script and AppSheet, which can interact with the Google Workspace API.

We covered a lot of ground in this section by talking about how to limit or grant access to third-party applications using OAuth scopes for more granular access control. These are powerful weapons in any administrator's arsenal and can help them defend a domain when a security war is raging.

Now, let's learn more about the friendly Google Assistant feature for Google Workspace.

## Google Assistant for Google Workspace

Most households have Google Assistant devices for voice-controlled actions. It could be as simple as "Hey Google, what's the weather?" or "OK Google, what sound does a cat make?"

Google Workspace can integrate with Google Assistant devices for a better user experience, allowing users to perform business actions using those Google Assistant devices.

These actions can include the following:

- Hey Google, when is my first meeting for the day?
- Hey Google, join my meeting
- OK Google, create a meeting
- OK Google, send an email to cancel the meeting

Administrators need to turn on Google Assistant in the Google **Admin** console. Users who have it can use their accounts to see personal results and access additional features. When you turn on Google Assistant, it will want other features to be turned on as well, such as Google Search, Assistant services, and Web & App Activity.

Administrators can also manage voice match and face match for users. Admins must get parental consent for users under the age of 18 to link their Google Workspace for Education accounts to a Google Assistant-enabled device to enable voice match and face match. Turning off voice match would mean that users may lose core features such as personalized results. Let's talk about how Google Assistant is enabled and integrated with consumer devices.

## Nest Hub

One of the most popular Google Assistant-enabled devices is Nest Hub. It comes in different sizes and is marketed as Nest Hub, Nest Hub Max, and Nest Mini:



Figure 5.22 – Google Nest Hub

Nest Hub integrates with Google Workspace seamlessly using the Google Nest Hub app, which is available as an additional Google service. Admins can mark this app as **Trusted** and allow it to be installed for users across a domain.

## Enabling the Search and Assistant service

As the next step, the administrator will have to enable the Search and Assistant service so that devices can interact with Google Workspace data using Google Assistant. To accomplish this, follow these steps:

1. Log into the Google **Admin** console.
2. Click on **Apps** from the left-hand side panel and select **Additional Google Services**.
3. Select **Search and Assistant**.
4. Enable this service for the specific OU or access groups for the user.

Once the service has been enabled, users can start using search features for this Google Workspace account:

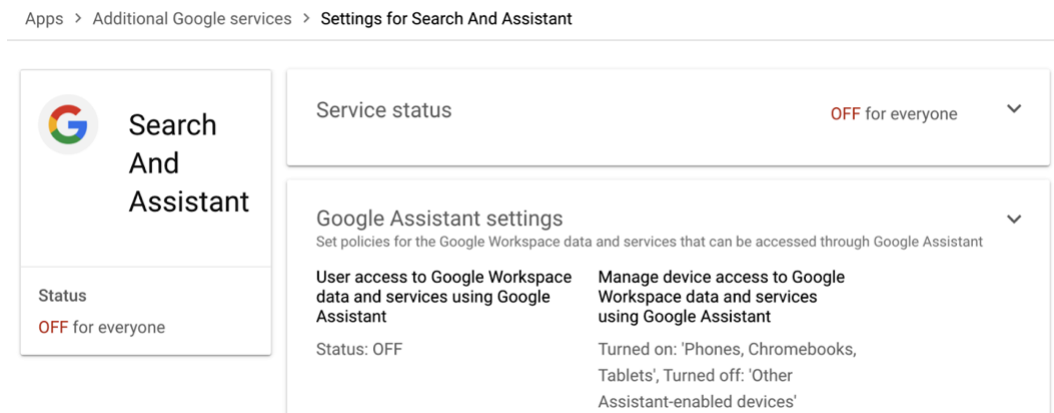


Figure 5.23 – Enabling the Search and Assistant feature

Furthermore, admins can also enable assistant devices to access Google Workspace data, as follows:

1. Log into the Google **Admin** console.
2. Click on **Apps** from the left-hand side panel and select **Additional Google Services**.
3. Select the **Search and Assistant** service.
4. Select **Google Assistant Settings**.
5. Enable the setting for **User access to Google Workspace data and services using Google Assistant**.
6. For the **Manage device access to Google Workspace data and services using Google Assistant** setting, select all the devices the organization wants to manage.
7. Click **Save**.

Now that searching across assistant devices has been enabled, administrators can enable **SafeSearch** for users to ensure that queries are indeed safe to use:

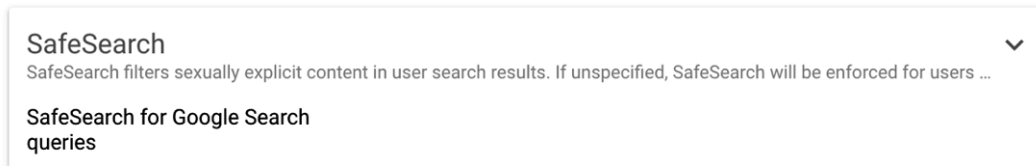


Figure 5.24 – SafeSearch enablement in the Google Admin console

Google Assistant can be very helpful as we all move toward using voice as a primary input form. Assistant's natural language processing is top-notch and can understand several languages and dialects. Google Assistant makes Workspace a joy to use.

With Google Assistant spoken for, let's move on and look at some popular third-party client integrations with Google Workspace.

## Using third-party clients

Google Workspace can be used on the web or on mobile devices. Users have an agile experience when connecting to Google Workspace data from anywhere, on any device, at any time. Services such as Gmail and Drive have offline capabilities that allow users to access Workspace data when there is no network connectivity.

If users would like to avoid web browsers and use a native mail client such as Thunderbird, Kiwi, or Apple Mail, the IMAP/POP3 setting must be enabled.

**IMAP** stands for **Internet Message Access Protocol** and uses internet standards to extract email messages from servers and display them on a local client.

**POP** stands for **Post Office Protocol** and uses standardized RFC-compliant methods to sync email messages from mail servers to local clients, such as Thunderbird and Apple Mail.

All actions, such as composing an email, sending an email, organizing emails into folders, and more, can be performed within the client. The emails that are sent using the client are synchronized with mailing servers. In this section, we will learn how to enable access for third-party mail clients and focus on a popular third-party client that can be used to access Google Workspace data.

## Enabling access for mail clients


IMAP and POP can be enabled individually. Furthermore, administrators can create an allowlist of clients that users can use to access their Google Workspace data.

These settings can be enabled selectively for a specific OU or access group. Nested OUs will inherit this configuration as well. To configure this option, follow these steps:

1. Log in to the Google **Admin** console.
2. Click on **Apps** from the left-hand side panel and select **Gmail**.
3. Click on **End User access**.
4. Select **POP and IMAP access** and turn on POP, IMAP, or both as appropriate for the domain.
5. Click **Save**.

- Enable IMAP access for all users  
[Learn more](#)
- Allow any mail client
- Restrict which mail clients users can use (OAuth mail clients only)

Comma separated list of OAuth client ids (maximum 20)

- Enable POP access for all users  
[Learn more](#)
-  Changes may take up to 24 hours to propagate to all users.  
Prior changes can be seen in [Audit log](#)

CANCEL SAVE

Figure 5.25 – Enabling IMAP and POP access

If the administrator creates an allowed list of clients to be used, the list of OAuth client IDs will have to be mentioned as well.

Some mail client applications require the **Less Secure Apps** setting to be enabled for a successful mail client setup. To enable this setting, follow these steps:

1. Log into the Google **Admin** console.
2. Click on **Security** from the left-hand side panel.
3. Select the **Less Secure Apps** configuration to allow or disable the use of such apps.
4. Click **Save**.

Once these settings have been configured in the Google **Admin** console, users can individually download their choice of mail client and set it up to use Google Workspace.

The following screenshot shows how to enable the **Less secure apps** setting:

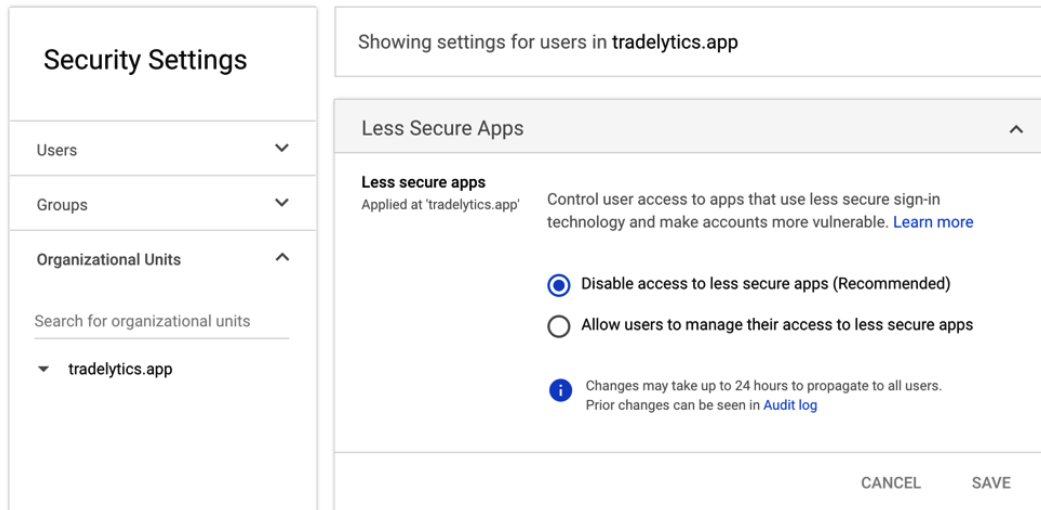


Figure 5.26 – Enabling the Less secure apps setting

#### Important Note

Caution must be exercised when enabling the **Less secure apps** setting as this can open a new attack vector and will make your Google Workspace settings less secure. Google's recommendation would be to switch to using a more secure authentication process for accessing apps, instead of turning this option on.



## Using Google Workspace Sync for Microsoft Outlook (GWSMO)

Now that we have reviewed the process of configuring various mail clients for accessing Google Workspace data, let's review the process of using Microsoft Outlook to access Google Workspace data:

1. Download and install GWSMO from <https://tools.google.com/dlpage/gssmo>.
2. Enter the appropriate username and password credentials to sign into the user's Google Workspace account.
3. Grant access for GWSMO to connect to this Google account.
4. Once GWSMO has been installed, import the data in one of the following ways:
  - From a PST file
  - Using an Outlook profile
  - Using a Microsoft Exchange profile

This will import Google Contacts, Calendar, and email messages from the connected Google Workspace account into the Microsoft Outlook client.

Once the import process is completed, users can use Google Workspace within Microsoft Outlook.

With third-party clients squared away, let's wrap this chapter up by looking at the accessibility features that are available in Google Workspace that makes this platform very inclusive.

## Accessibility for users

Google Workspace has been designed with users being the primary focus. The mission is to make the product accessible for all users, including people with disabilities, such as those with color vision deficiency and visual and hearing impairment. Google has been building accessibility into their products and Google Workspace is no exception.

To make it easier for organizations to comply with Accessibility standards, a **Voluntary Product Accessibility Template (VPAT)** is available for several Google Workspace services:

- Calendar VPAT: <<https://static.googleusercontent.com/media/www.google.com/en//accessibility/static/pdf/google-calendar-vpat.pdf>>
- Gmail VPAT: <[https://services.google.com/fh/files/misc/gmail\\_vpat.pdf](https://services.google.com/fh/files/misc/gmail_vpat.pdf)>

The accessibility features include screen reader compatibility, a larger font for the user interface, enabling IMAP/POP to allow users to use their choice of mail client, braille device compatibility, and more.

## Summary

This chapter provided you with a glimpse of how Google helps students and educational institutions with Google Classroom. Although various learning management and collaboration platforms exist, no one comes closer to offering services like Google at a global scale. More interestingly, to make Google Classroom more accessible, Google gives away its basic version for free, which is sufficient for a lot of educational institutions. While there are some negative reviews about the simplicity of the Google Classroom UI and its workflow, Classroom continues to evolve and will reshape the educational landscape across the globe.

We also saw how Google Workspace services can be extended beyond the services offered by Google, a true differentiator in the market with these Marketplace apps and add-on functionalities. Google Assistant and its integration with Google Workspace turns mundane activities such as setting up a calendar into a delight with voice inputs. Personalized search results for users means that every user gets an assistant, unleashing the full potential of voice-assisted services whose feature set continues to grow.

Google's commitment to making information available across all users is well etched into its accessibility capabilities. People with impairments can access almost all Workspace services and enjoy its benefits.

In the next chapter, we will dive into developing custom applications that will automate your unique business processes using Apps Script and Workspace API.